AFRL-SA-WP-TR-2013-0006

Sources of Occupational Stress and Prevalence of Burnout and Clinical Distress Among U.S. Air Force Cyber Warfare Operators

Wayne Chappelle, Psy.D., ABPP[1]
Kent McDonald, Col, USAF, MC, FS[1]
James Christensen, Ph.D.[2]
Lillian Prince, M.S.S.I.[3]
Tanya Goodman, M.A.[4]
William Thompson, M.A.[4]
William Hayes, Maj, USAF, MC, FS[1]

[1]Neuropsychiatry Branch, USAFSAM, Wright-Patterson AFB, OH
[2]Applied Neuroscience Branch, AFRL, Wright-Patterson AFB, OH
[3]SpecPro Technical Services, LLC, USAFSAM, San Antonio, TX
[4]NeuroStat Analytical Solutions, LLC, USAFSAM, San Antonio, TX

January 2013

Final Report
for October 2011 to April 2012

Distribution A: Approved for public release; distribution is unlimited.
Case Number: 88ABW-2013-2089,
3 May 2013

Air Force Research Laboratory
711th Human Performance Wing
School of Aerospace Medicine
Aerospace Medicine Department
Neuropsychiatry Branch
2510 Fifth St.
Wright-Patterson AFB, OH 45433-7913

NOTICE AND SIGNATURE PAGE

Using Government drawings, specifications, or other data included in this document for any purpose other than Government procurement does not in any way obligate the U.S. Government. The fact that the Government formulated or supplied the drawings, specifications, or other data does not license the holder or any other person or corporation or convey any rights or permission to manufacture, use, or sell any patented invention that may relate to them.

Qualified requestors may obtain copies of this report from the Defense Technical Information Center (DTIC) (http://www.dtic.mil).

AFRL-SA-WP-TR-2013-0006 HAS BEEN REVIEWED AND IS APPROVED FOR PUBLICATION IN ACCORDANCE WITH ASSIGNED DISTRIBUTION STATEMENT.

//SIGNATURE//

COL LEE BEYER, Chief FEC
Chief, Aerospace Medicine Consult Div

//SIGNATURE//

COL ROBERT E. CARROLL
Chair, Aerospace Medicine Department

This report is published in the interest of scientific and technical information exchange, and its publication does not constitute the Government’s approval or disapproval of its ideas or findings.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)* 1 Jan 2013	**2. REPORT TYPE** Final Technical Report	**3. DATES COVERED *(From – To)*** Oct 2011 – Apr 2012

4. TITLE AND SUBTITLE

Sources of Occupational Stress and Prevalence of Burnout and Clinical Distress Among U.S. Air Force Cyber Warfare Operators

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Wayne Chappelle, Kent McDonald, James Christensen, Lillian Prince, Tanya Goodman, William Thompson, William Hayes

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

USAF School of Aerospace Medicine
Aerospace Medicine Dept/FECN
2510 Fifth St.
Wright-Patterson AFB, OH 45433-7913

8. PERFORMING ORGANIZATION REPORT NUMBER

AFRL-SA-WP-TR-2013-0006

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSORING/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Distribution A: Approved for public release; distribution is unlimited. Case Number: 88ABW-2013-2089, 3 May 2013

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The continual need to sustain a constant high operational tempo in response to real-time threats to cyber operations critical to U.S. Air Force operations has raised concerns among commanders (i.e., line and medical leadership) regarding the prevalence of occupational burnout and clinical distress among this critical workforce. The purpose of this study is to identify the main sources of occupational stress and prevalence of burnout and clinical distress within the cyber warfare community. This study involved cyber warfare operators including active duty (n = 376) and civilian contractor and Department of the Air Force Government personnel (n = 156) at Air Force installations within the continental U.S. This study also included airmen from logistics/support units (n = 795) from continental U.S. units to serve as a control-comparison group. Participants in the study completed a web-based self-report occupational health stress screening that included: (a) demographic and background questionnaire, (b) qualitative open-ended items asking respondents to describe their top sources of occupational stress, (c) the Maslach Burnout Inventory, and (d) the Outcome Questionaire-45.2. Results revealed that when compared to civilian cyber warfare operators, active duty cyber warfare operators are more likely to suffer from the facets of occupational burnout involving emotional exhaustion and cynicism and are at increased risk for clinical distress. Qualitative analyses of respondents' write-in responses revealed cyber warfare operators attributed shift work, shift changes, and hours worked as the primary sources of high occupational stress. Cyber warfare stressors (such as attacking adversarial networks or defending Government cyber networks from real-time attacks) were not listed as primary stressors. Recommendations to leadership and medical personnel to mitigate burnout and clinical distress among cyber warfare operators are discussed.

15. SUBJECT TERMS

Cyber warfare operators, occupational burnout, clinical distress, shift work, occupational stressors, emotional fatigue

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON** Dr. Wayne Chappelle
a. REPORT U	**b. ABSTRACT** U	**c. THIS PAGE** U	SAR	26	**19b. TELEPHONE NUMBER *(include area code)***

This page intentionally left blank.

TABLE OF CONTENTS

Section **Page**

TABLE OF CONTENTS (concluded)

Section **Page**

1.0 EXECUTIVE SUMMARY

The need for sustained 24/7 offensive and defensive cyber warfare operations has led to concerns regarding increased occupational stress for those who conduct these missions. The continual need to sustain a constant high operational tempo in response to real-time threats to cyber operations critical to U.S. Air Force operations has raised inquiries among commanders (i.e., line and medical leadership) regarding the prevalence of occupational burnout and clinical distress among this critical workforce. Currently, no published studies exist that evaluate the impact of occupational stressors and the prevalence of burnout and clinical distress within the cyber warfare community. The purpose of this study is to fill the gap in the literature by examining such issues.

This study involved cyber warfare operators including active duty (n = 376) and civilian contractor and Department of the Air Force government personnel (n = 156) at Air Force installations within the continental U.S. This study also included airmen from logistics/support units (n = 795) from continental U.S. units to serve as a control-comparison group.

Participants in the study completed a web-based self-report occupational health stress screening assessment. The assessment included (a) demographic and background questionnaire, (b) qualitative open-ended items asking respondents to describe their top sources of occupational stress, (c) the Maslach Burnout Inventory for measuring the facets of occupational burnout, and (d) the Outcome Questionaire-45.2 to measure clinical levels of distress. Both measures of burnout and clinical distress are commercially available, standardized instruments.

Results revealed that when compared to civilian cyber warfare operators, active duty cyber warfare operators are more likely to suffer from the facets of occupational burnout involving emotional exhaustion and cynicism and are at increased risk for high levels of clinical distress. Qualitative analyses of respondents' write-in responses revealed that cyber warfare operators attributed shift work, shift changes, and hours worked as the primary sources of their high occupational stress. Cyber warfare stressors (such as attacking adversarial networks or defending government cyber networks from real-time attacks) were not listed as primary stressors. Recommendations to leadership and medical personnel to mitigate the risk of burnout and clinical distress among cyber warfare operators are discussed.

2.0 INTRODUCTION

In recent years, the U.S. Air Force (USAF) has significantly expanded the scope of its cyberspace mission. The expansion into cyber warfare has transformed the mission and objectives of the USAF to be able to obtain superiority within an electromagnetic arena and space, commonly referred to as cyberspace. Over the past 5 years, the USAF has focused efforts on fostering a force of 21st century warriors capable of delivering a full array of kinetic and nonkinetic, lethal and nonlethal cyberspace effects within a highly organized warfighting architecture [1,2]. USAF resources have been devoted to establishing a cyberspace command structure focused on developing the manpower, capabilities, and techniques for achieving such goals. Since military and government operations, as well as acts of war, have become increasingly dependent on cyberspace operations, USAF cyber warfare operators must be capable of supporting component as well as joint force operations across this unique spectrum of warfare on a continual, around-the-clock basis (Rector J. Personal communication; 2012).

Cyber operations encompass a variety of technologies configured across multiple networks to perform a broad array of functions. Within the spectrum of cyberspace missions, the same technologies may be employed across multiple mission areas and network architectures to achieve highly varied and distinctly defined operational goals. Whether supporting offensive or defensive missions, cyber operations involve constantly changing technologies, demand ever-present vigilance, and require a highly trained and dynamic work force.

Successful cyber warfare operations are executed by a team of cyber warfighting professionals who establish, control, and project combat power in and through cyberspace. This team of warfighting operators is organized into a series of units and organizations with specific functions that include cyber attack, cyber defense, and cyber exploitation (see section 2.1 for more details on these specific functions). Their duties include employing up-to-date, real-time, cyber techniques, tools, and systems. Individual responsibilities within units and organizations can vary, depending on the scope and the position within cyberspace that an operator is assigned to attack, defend, or exploit. Those who support cyber warfare operations are divided as follows:

- cyber operators: officer and enlisted members who plan, direct, and execute offensive and defensive actions
- specialists: enlisted communications and information personnel who specialize in technical aspects of cyberspace
- analysts: officer and enlisted intelligence personnel with the technical foundations to support cyberspace operations
- developers: primarily officers and enlisted members with advanced skills for designing and modifying software and hardware packages

Interviews the authors of this study have had with several cyber commanders at the squadron level reveal a significant increase in operational hours, shift work, and an unending surge of cyber warfare tasks levied upon certain cyber units. As a result of the continual need to sustain an “around-the-clock” 24/7 high operational tempo, there are concerns among line and medical leadership regarding the prevalence of occupational burnout and clinical distress among those having to sustain offensive, defensive, and exploitation missions.

Furthermore, interviews with several cyber commanders indicate reasons for concern the the level of stress, specifically occupational burnout, may be significantly higher for active duty than civilian (contractor or government personnel) cyber warfare operators. All cyber warfare operators must contend with having to simultaneously manage a high operational tempo while juggling their role as a cyber warrior with their domestic duties. However, there is concern that active duty operators may work longer hours, have more frequent shift changes, and struggle with more career-oriented stressors than civilian operators working within the same units. Active duty operators must also contend with military-specific training and deployment issues. They are also more readily available to work longer hours during manning shortages because there are less restrictions upon supervisors regarding how they are utilized.

Research has revealed a significant amount of problems associated with occupational burnout such as increased occupational stress [3-5]; decreased professional identity [6]; reduced personal accomplishment and depersonalization [7]; significant feelings of role conflict, group, and political pressures; and underparticipation [4] in occupational initiatives. However, there is an insufficient amount of literature and objective information available regarding the impact of such operations on the emotional well-being of cyber warfare operators.

2.1 USAF Cyber Warfare Operators

Cyber warfare operators employ a variety of cyber weapon strategies, tools, and systems to enable access, escalate privileges, ex-filtrate data, and deliberately disrupt cyberspace operations [2]. The focus of this study is on those cyber operators who engage in cyber warfare, along with any support and sustainment responsibilities that may be levied upon them. Cyber warfare operations are divided into computer network attack, computer network defense (CND), and computer network exploitation (CNE). Each role is described in more detail below.

Computer attack operations are actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves [8]. Operators performing attack operations must understand the diverse forms of technology and functions of adversarial target systems. Understanding the forms and function of specific adversarial systems is key to knowing how, when, and where to put "effects on target." To remain effective, personnel performing attack operations must maintain combat-mission-ready status qualifications in these cyber-based weapons systems and tools, as well as a high level of expertise in the technologies and functions of the adversary networks and systems they target.

Network defense operations involve actions taken through the use of computer networks to protect, monitor, analyze, detect, and respond to unauthorized activity within Department of Defense information systems and computer networks [8]. Operators are assigned to missions of defense and control of specified portions of cyberspace, which can range from a simple local area network within a single facility or airborne platform to an entire global network [2]. Regardless of the scope of responsibility, operators must be experts in the function of the platform they are tasked with protecting. To defend a complex network effectively, a CND team must understand both the technologies and functions (i.e., the mission it supports) of the networks. CND operators at the tactical level may manage perimeter network sensors to defend against unauthorized attempts to access a network, while those at the operational level may direct large-scale, dynamic configuration changes in response to adversary attacks [2]. Regardless, each defense technician must be skilled in the technologies and functions of his or her area of expertise and operate in accordance with mission priorities and defensive strategies established for the defended network [2]. It is important to note that cyberspace threats upon military and government systems have graduated beyond attacks against common administrative networks and websites to critical infrastructure resources, such as air traffic control and utility-managing supervisory control and data acquisition systems [2].

Exploitation operations are enabling operations and intelligence collection capabilities conducted with computer networks to gather data from target or adversary automated information systems or networks. CNE operators are involved with monitoring adversary activities and gathering information through cyber operator methods and resources. For example, CNE operators include analytic and targeting specialists who fuse all-source intelligence to analyze adversary networks and prepare offensive targeting solutions for cyber warfare weapons and tools. Due to the shared skill sets, CNE is often closely integrated with computer network attack. Additionally, CNE operators are tasked with maintaining engineering and software-development skills to aptly construct new (or modify existing) attack and defense strategies, tools, and systems.

2.2 Cyber Warfare Operator Occupational Stressors

There is a wide range of occupationally oriented stressors that cyber warfare operators experience that may result in negative changes to their emotional well-being. These stressors may vary across duty positions, geographical location, unit mission, as well as status (i.e., active duty, civilian). An extensive list of such stressors is beyond the scope of this study. However, below is a list of perceived stressors obtained from discussions the authors of this study have had with cyber command leadership and USAF medical personnel. The stressors are separated into three conceptual categories: operational, warfare oriented, and career oriented.

Operational stressors are defined as those related to sustaining operations. These operational stressors include issues such as available manpower, equipment, and general resources. There are several important operational stressors to consider when assessing the risk of occupational burnout among cyber warfare operators, including, but not limited to:

- chronic, long work week hours (50 or more hours) over long periods of time to accomplish task requirements
- rotating shift work requirements that make it difficult to maintain domestic life routines
- restricted working environment that limits personal mobility and rest breaks
- poorly designed work stations and ergonomics not well suited or tailored to maximize performance
- constant need to sustain high levels of vigilance to a visual workload and multitasking with time-limited suspenses

It stands to reason such stressors can lead to both physical and psychological distress when faced on a daily basis. The long hours combined with rotating shift work can reasonably elevate the risk of occupational fatigue that is accentuated by difficulty with maintaining a routine domestic life.

Cyber-warfare oriented stressors are defined as those related to the direct engagement in warfare-oriented tasks. Such operators must contend with a continuous cyberspace battleground with unending surges in tasks to defend, attack, and exploit. The continuous demand is accentuated by the exponential and rapid growth in technological advancements. Just as a new strategy is developed or intercepted, and then mastered, a far more advanced maneuver, software program, and other technical capabilities are under development and implemented by adversarial agents. Cyber warfare stressors that may lead to occupational burnout include, but are not limited to:

- *high pressure*, such as the daily, high-pressure, real-time suspenses to thwart adversarial, malicious attacks on networks
- *sustaining progress* with techniques and capabilities in a rapidly and constantly evolving technological environment
- *sustaining continual expertise* in the rapidly changing technologies and functions of adversary networks and systems
- *sustaining situational awareness* of the assortment of functions constructed with a mix of commercially available and proprietary technologies that may be exploited by adversarial agents

- *ubiquitous, cyber threats* regarding the realization that many adversarial cyber threats are ever present, requiring operators to continually race to expand their scope of capabilities within their assigned cyberspace domain
- *pressure to maintain top secret information* associated with the daily, constant pressure to compartmentalize and protect disclosure of their cyber warfare mission from their domestic life and responsibilities

Career-oriented stressors are those associated with training, advancement, and promotion within a military arena and specific career field (Rector J. Personal communication; 2012). The cyber warfare career field is relatively new in contrast to many others within the USAF and Department of Defense. Aspects regarding competitive career progression and promotion in cyber warfare operations may appear uncertain for active duty members. The expansion into cyberspace is a relatively new arena in contrast to USAF history and culture. Newly established organizational structure can also be associated with challenges in clear lines of doctrine, policy, and training issues. Although the USAF has made a concerted effort to develop cyber warfare skill sets, career field, and identity, current cyber warriors serve only as the first generation of what must inevitably become a much more diverse field of professionals [2]. As a result, current cyber warfare operators may struggle with a defined culture, sense of identity, and clear promotional paths within a military branch traditionally associated with air and space power. Furthermore, it is likely the expansion of cyber warfare operations has resulted in a significant percentage of inexperienced operators in need of mentorship and guidance from more experienced, senior operators. Simply put, there may not be enough experienced operators to provide the amount of guidance and mentorship needed.

2.3 Medical Concerns Regarding Cyber Warfare Operators

Occupational performance within a high-demand, high-operational environment requires a healthy state of physical and psychological functioning. According to USAF medical policy, if cyber warfare operators suffer from physical or psychological conditions that are reasonably perceived to lead to degradation in performance, then they are disqualified from participation in their warfare duties. Although occupational burnout is not a categorical psychiatric diagnosis, research demonstrates that such a condition leads to performance degradation and, if untreated, may lead to significant emotional difficulties and increased occupational stress [3-6].

Occupational burnout has been studied in depth and defined by Maslach, Jackson, and Leiter [9] as containing three aspects: (1) emotional exhaustion (i.e., depletion of emotional energy and reserves due to work-related stress), (2) cynicism (a sense of indifference or a distant attitude toward work, as well as declining sense of enthusiasm for work), and (3) personal efficacy (i.e., a sense of satisfaction with accomplishments and efficacy at work). Occupational burnout is composed of high levels of emotional exhaustion and cynicism, combined with low levels of personal efficacy. Consequently, the negative effects of occupational burnout can be wide ranging, from impaired ability to complete tasks to difficulty relating to people.

Furthermore, emotional distress is a common phrase used to refer to an unpleasant emotional state characterized by negative emotional (e.g., anger, irritability, anxiety, sadness), behavioral (e.g., arguments with family members, difficulty getting along with others), physical (e.g., difficulty sleeping, fatigue, headaches), and cognitive (e.g., difficulty concentrating, sustaining attention) changes in functioning. Given the critical nature of cyber warfare operations, it is important to military commanders to gauge the levels of emotional distress experienced among such operations. If a significant portion of cyber warfare operators is found to be experiencing high levels of distress, the commanders and medical providers may realize a need for intervention to preserve the performance and well-being of airmen under their command (Bachman R. Personal communication; 2012).

2.4 Study Purpose

USAF medical personnel and line leadership must make concerted efforts to evaluate occupational stress, as well as mitigate occupational stressors to optimize the cyber warfare operator's performance. The purpose of this study is to:

- assess self-reported occupational stressors among cyber warfare operators
- evaluate facets of occupational burnout (high emotional exhaustion, high cynicism, and low sense of professional efficacy) among cyber warfare operators
- evaluate clinical levels of distress among such operators and prevalence of those at high risk for the development of emotional difficulties
- assess for differences between active duty and civilian cyber warfare operators on such measures of stress

3.0 METHODS

3.1 Participants

Participants included active duty military, government civilian, and contract personnel assigned to cyber warfare operations. *The purpose and methodology of the study were reviewed and granted exemption from the Wright-Patterson Air Force Base Institutional Review Board and assigned protocol number F-WR-2011-0068-E. The voluntary and fully informed consent of participants was obtained.*

3.1.1 Active Duty Cyber Warfare Operators. There were 376 active duty cyber warfare operator participants constituting 68.11 % of the overall sample group. Among the active duty participants, there were 303 males (80.6%) and 68 females (18.4%). There were 207 (55.0%) between the ages of 18-30, 140 (37.2%) between the ages of 31-39, and 26 (7.0%) 40 years of age or older. The sample was composed of 99 (26.3%) airmen (E1-E4), 156 (41.5%) noncommissioned officers (E5-E6), 52 (13.8%) senior noncommissioned officers (E7-E9), 57 (15.2%) company grade officers (O1-O3), and 9 (2.4%) field grade officers (O4-O6). Three active duty participants did not report their rank, and 4 participants did not report age. A total of 117 (31.1%) reported being single, and 226 (60.1%) reported being married. Twenty-six active duty participants reported being in unmarried relationships or in a state of marital transition (i.e., divorce/separation). Twelve participants did not report their marital status. A total of 206 (54.8%) of the participants reported having children living at home, and 76 (20.2%) denied having children living at home.

3.1.2 Civilian/Contract Cyber Warfare Operators. There were 156 civilian/contract cyber warfare operator participants constituting 28.26% of the overall sample group. Among these participants, there were 127 males (81.4%) and 27 females (17.3%); 24 (15.4%) were between the ages of 18-30, 24 (15.4%) between the ages of 41-40, and 106 (67.9%) age 40 and older. Among these participants, 2 (1.3%) did not report their age. A total of 45 (28.8%) reported being single, and 107 (68.6%) reported being married. Four participants did not report their marital status. A total of 84 (53.8%) reported having children living at home, 35 (22.4%) denied having children living at home, and 37 (23.7%) elected to not share details on their dependent children.

3.1.3 Control Group. There were 795 active duty control group participants from multiple, noncyber, support, and logistics squadrons. This group serves as a comparison group representing the vast majority of airmen who serve at installations within the United States. Most airmen are from logistics and support squadrons and thereby represent a typical, common group of USAF airmen for baseline comparison. This group does not include aircrew, special duty operators, or security forces who represent a more unique group of airmen. Among the participants, there were 684 males (86.5%) and 107 females (13.5%); 596 (76%) were between the ages of 18-30, 169 (21.3%) between the ages of 31-40, and 27 (3.4%) over the age of 40. There were 75 (9.4%) airmen (E1-E4), 102 (12.8%) noncommissioned officers (E5-E6), 291 (36.6%) senior noncommissioned officers (E7-E9), 252 (31.7%) company grade officers (O1-O3), and 70 (8.8%) field grade officers (O4-O6). A total of 339 (42.6%) reported being single, and 435 (54.7%) reported being married. Three participants did not report their marital status. A total of 326 (41%) reported having children living at home, and 469 (59%) either denied having children living at home or elected to not share details on their dependent children.

3.2 Measures

Participants were given a web-based survey composed of items that asked about rank range, gender, age range, marital status, length of time serving as a cyber warfare operator, average number of hours worked in a typical week, current work shift, and sources of occupational stress. The demographics questionnaire was developed to allow participants to remain anonymous to increase self-disclosure in a community in which there is strong cultural stigma regarding physical and emotional difficulties.

3.2.1 Maslach Burnout Inventory-General Schedule (MBI-GS). The MBI-GS is a leading measure that assesses the facets of occupational burnout. The self-report measure is a 16-item questionnaire that assesses occupational burnout [9]. As mentioned previously, occupational burnout is a syndrome composed of high levels of emotional exhaustion and cynicism, with low levels of personal efficacy. Consequently, the negative effects of occupational burnout can be wide ranging, from impaired ability to complete tasks to difficulty relating to people. The emotional exhaustion and cynicism subscales are each composed of five items, and the professional efficacy subscale is composed of six items. Construct validity of the MBI-GS has been established through principal component analyses with other constructs for each of the scales. Stability coefficients range from .65 to .67 [9].

3.2.2 Outcome Questionnaire-45.2 (OQ-45.2). The OQ-45.2 is a 45-item self-report questionnaire assessing symptoms of emotional distress [10]. The survey includes items that assess emotional difficulties (e.g., anxiety, depression, anger, suicidal ideation), occupational difficulties (e.g., performance problems, stress, and relational conflict at work, in relationships), and general quality of life. Each item has a Likert response rating from “Almost Always” to “Never.” The responses are numerically coded on a scale of 0 to 4 based upon the direction of endorsement. The items are summed to yield a total emotional distress score. Several items are reverse-scored to reduce random responding. The 45-item questionnaire has a score range of 0 to 180. A total score cut-off of 63 or more indicates high levels of emotional distress [10]. The OQ-45.2 also has a Social Role distress subscale. This subscale measures symptoms of conflict at with others at work and adjustment-related difficulties and symptoms with work role adjustments. This subscale is logically perceived to evaluate those whose stress is interfering with their performance, satisfaction, and interactions with others at work. Concurrent validity estimates for the total score range from .64 to .88. Test-retest reliability and internal consistency values for the OQ-45.2 total score range from .84 to .93. The OQ-45.2 is commonly used at mental health clinics on USAF installations to assess distress and track progress among USAF personnel seeking mental health care.

3.3 Procedure

The demographic questions, MBI-GS, and OQ-45.2 were placed into an electronic web-based format as a single, comprehensive health assessment on occupational stress. The web-based survey was placed on a controlled internet site with an established on-line link. Leadership (group, squadron, and flight commanders from active duty units) sent an email with a request to participate in an anonymous, voluntary study. Cyber warfare operators who chose to voluntarily participate in the study were provided the on-line link to the web-based survey that they could access from their work station computer. The voluntary and anonymous nature of participation to the web-based survey was emphasized in the e-mail request to support genuine and honest disclosure. The standardized e-mail request included statements that participation was encouraged to better understand the main sources of stress and levels of stress so leadership would be equipped to initiate changes that could lead to improvements in health and morale. The web-based format of the survey provided easy and discrete access for all participants. In general, it took participants 25 to 30 minutes to complete all the items on the survey.

4.0 RESULTS

4.1 Response Rates

A total of 7 squadrons participated in the survey, representing the vast majority of continental U.S. units. Response rates ranged from 25% to 72%, with an average response rate of 40%.

4.2 Occupational Stressors

Participants’ qualitative, self-reported, write-in responses to the item asking them to describe their top three sources of occupational stress were analyzed. A total of three behavioral science researchers performed a qualitative analysis on the content of participant responses. Each research team member consolidated qualitative responses into a list of specific categories. Responses that appeared to label the same or similar stressors were consolidated under a single category. For example, terms such as “rotating shift schedule every 30 days” and “switching from day to swing shift” were categorized under the main stressors of shift work. The categories were then ranked according to the number of participants who endorsed stressors within each category. The top four categories with the most number of endorsements from survey participants were singled out. Refer to Table 1 for the results of the analyses.

Table 1. Top 4 Sources of Occupational Stressors Rated by Cyber Warfare Operators[a]

Ranking	Cyber Warfare Operator		Noncyber Operator AF Control Group Stressors
	Active Duty Stressors	**Civilian/Contractor Stressors**	
1	**LEADERSHIP/ORGANIZATIONAL ISSUES** (e.g., leaders not communicating requirements, inexperienced cyber leadership not understanding operational needs/realities)	**LEADERSHIP/ORGANIZATIONAL ISSUES** (e.g., leaders not communicating requirements, inexperienced cyber leadership not understanding operational needs/realities)	**FINANCIAL CONCERNS** (e.g., economic concern over fiscal cutbacks on resources for active duty)
2	**OPS TEMPO/WORKLOAD/MANNING** (e.g., insufficient manning, overwork with little recognition, frequent short-notice, line-of-sight tasking, constant 50+-h work weeks)	**OPS TEMPO/WORKLOAD/MANNING** (e.g., insufficient manning, overwork with little recognition, frequent short-notice, line-of-sight tasking, constant 50+-h work weeks)	**CAREER PROGRESSION** (e.g., access to training & organizational activities leading to on-time promotion)
3	**NATURE OF WORK & TRAINING** (e.g., inadequate tools & training, lack of experienced operators to provide training & mentorship, challenge of keeping up with rapidly changing technology)	**JOB SECURITIY/FINANCIAL CONCERN** (e.g., economic worries associated with temporary nature of contract work, risk of job/pay loss at contract renewal time)	**FITNESS** (e.g., sustaining regular exercise program, meeting fitness standards, access to fitness resources)
4	**SHIFT WORK** (e.g., effects of shift work on family & life obligations, stress caused by rotating shifts, family care complications due to shift work, lack of time spent with family)	**NATURE OF WORK & TRAINING** (e.g., inadequate tools & training, lack of experienced operators to provide training & mentorship, challenge of keeping up with rapidly changing technology)	**OCCUPATIONAL MORALE**(e.g., engaging in activities to promote communication, team-building, job satisfaction)

[a] Although the main occupational stressors were the same for active duty and civilian/contractor cyber warfare operators, it’s important to note that many contractor cyber operators reported concerns with fiscal cutbacks that would result in a force reduction and loss of job.

4.3 Emotional Exhaustion-Fatigue

The mean emotional exhaustion scale from the MBI-GS score per group was 13.42 (standard deviation (SD) = 7.78) for cyber active duty operators, 10.30 (SD = 7.58) for cyber civilian/contractor operators, and 10.07 (SD = 7.68) for the noncyber control group. An analysis of variance assessing between group differences was significant, F = 23.5, p < 0.01. Subsequent mean comparisons using t-tests for equal variance (Bonferroni t) were significant when comparing mean scores between cyber active duty and civilian/contractor (t = 3.11, p < 0.01) operators as well as between cyber active duty operators and the AF noncyber control group (t = 3.34, p < 0.01). There was no significant difference between the cyber civilian/contractor group and the noncyber control group.

The number and percentage of those in each group who had an emotional exhaustion score of 20 or higher (a discretionary cut-off score set by the authors of this study to be considered indicative of high emotional exhaustion) were 91 (25.78%) for cyber active duty operators, 22 (14.86%) for cyber civilian/contractors, and 107 (13.99%) for the noncyber control group (see Figure 1). Subsequent chi-square tests assessing for differences in frequencies in each group regarding those who reported high levels of exhaustion were significant between cyber active duty and cyber civilians/contractor (χ_2 = 7.11, $p < 0.01$) operators and between cyber active duty and the noncyber control group (χ_2 = 23.05, $p < 0.01$). There was no statistical difference between cyber civilian/contractor operators and the noncyber control group (χ_2 = 0.08, $p < 0.78$).

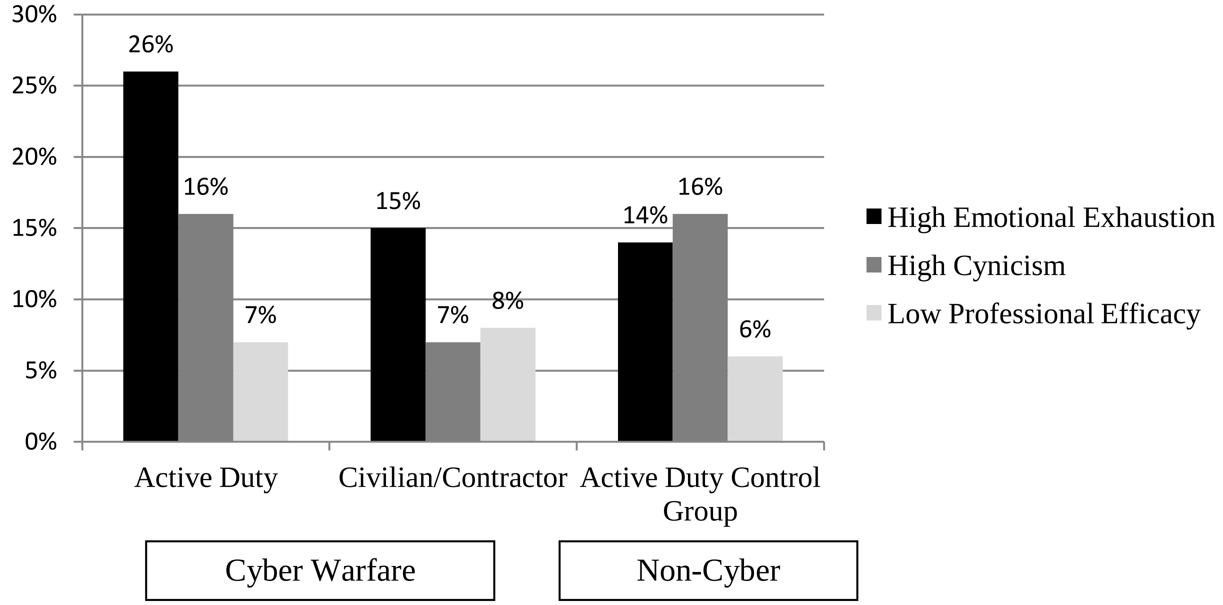

Figure 1. Percentage of Personnel Per Group that Endorsed Critical Cut-Off Scores for the Scales of the MBI-GS

4.4 Cynicism

The mean MBI-GS occupational cynicism scale score per group was 10.65 (SD = 7.82) for active duty cyber operators, 8.31 (SD = 7.13) for cyber civilian/contractor operators, and 10.25 (SD = 7.90) for the noncyber control group. An analysis of variance assessing between group differences was significant, F = 4.93, $p < 0.01$. Subsequent mean comparisons using t-tests for equal variance (Bonferroni t) were significant when comparing mean scores between active duty cyber operators and cyber civilian/contractor operators (t = 2.34, $p < 0.01$) and between cyber civilian/contractor operators and the noncyber control group (t = 1.94, $p < 0.01$). There was no significant difference between active duty cyber operators and the noncyber control group.

The number and percentage of those in each group who had a cynicism scale score of 20 or higher in each group (a discretionary cut-off score set by the authors of this study to be considered indicative of a high level of cynicism) were 56 (15.86%) for cyber active duty operators, 10 (6.76%) for cyber civilian/contractor operators, and 121 (15.67%) for the noncyber control group (see Figure 1). Subsequent chi-square analyses to assess for differences between groups regarding the frequency of those reporting high levels of cynicism were significant between cyber active duty and cyber civilian/contractor operators ($\chi_2 = 7.56$, $p < 0.01$) and between cyber civilian/contractor operators and the noncyber control group ($\chi_2 = 8.09$, $p < 0.01$). There was no statistical difference between active duty cyber operators and the noncyber control group ($\chi_2 = 0.01$, $p < 0.94$).

4.5 Professional Efficacy

Overall, the mean MBI-GS professional efficacy scale score per group was 23.80 (SD = 7.45) for active duty cyber operators, 26.23 (SD = 8.02) for cyber civilian/contractor operators, and 25.38 (SD = 7.75) for the noncyber control group. An analysis of variance assessing between group differences was significant, F = 7.04, $p < 0.01$. Subsequent mean comparisons using t-tests for equal variance (Bonferroni t) were significant when comparing mean scores between active duty cyber operators and cyber civilian/contractor operators (t = -2.43 $p < 0.01$) and between active duty cyber operators and the noncyber control group (t = -1.58, $p < 0.01$). There was no significant difference between cyber civilian/contractor operators and the noncyber control group (t = 0.85, $p <0.66$).

The number and percentage of those who had professional efficacy scale scores of 12 or lower (a discretionary cut-off score set by the authors of this study to be considered indicative of a low level of professional efficacy) were 24 (6.82%) for active duty cyber operators, 11 (7.48%) for cyber civilian/contractor operators, and 43 (5.61%) for the noncyber control group (see Figure 1). Subsequent chi-square tests assessing for differences in frequencies in each group regarding those who reported low levels of professional efficacy were not significant between active duty cyber operators and cyber civilian/contractor operators ($\chi_2 = 0.07$, $p < 0.79$). There was also no statistical difference between active duty cyber operators and the noncyber control group ($\chi_2 = 0.63$, $p < 0.43$) or between cyber civilian/contractor operators and the noncyber control group ($\chi_2 = 0.78$, $p < 0.38$).

4.6 OQ-45.2 – Overall

Overall, the mean OQ-45.2 total score per group was 40.39 (SD = 20.33) for active duty cyber operators, 38.11 (SD = 20.32) for cyber civilian/contractor operators, and 35.77 (SD = 20.07) for the noncyber control group. An analysis of variance assessing between group differences was significant, F = 6.06, $p < 0.01$. Subsequent mean comparisons using t-tests for equal variance (Bonferroni t) were significant only when comparing mean scores between active duty cyber operators and the noncyber control group (t = 4.62, $p < 0.01$). There was no significant difference between cyber civilian/contractor operators and the noncyber control group (t = 2.33, $p <0.62$).

The number and percentage of those per group who had an OQ-45.2 total score of 63 or more (a discretionary cut-off score set by the authors of the measure of the OQ-45.2 as indicative of high clinical distress) were 53 (15.06%) for active duty cyber operators, 17 (11.64%) for cyber civilian/contractor operators, and 59 (9.05%) for the noncyber control group (see Figure 2). Subsequent chi-square tests assessing for differences in frequencies in each group regarding those who reported high levels of clinical distress showed no significance between active duty cyber operators and cyber civilian/contractor operators ($\chi_2 = 1.00$, $p < 0.32$) or between cyber civilians/contractor operators and the noncyber control group ($\chi_2 = 0.93$, $p < 0.33$). However, there was a statistically significant difference between active duty cyber operators and the noncyber control group ($\chi_2 = 8.32$, $p < 0.01$).

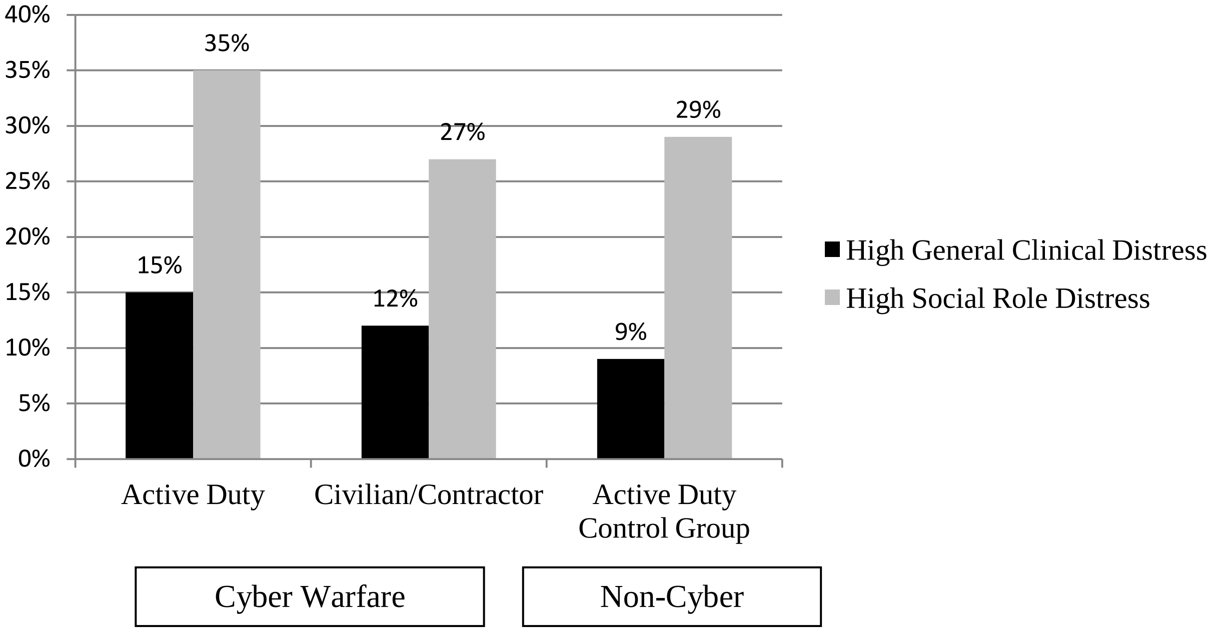

Figure 2. Percentage of Personnel Per Group that Endorsed Critical Cut-Off Scores for the Total Scale Score (General Clinical Distress) and Social Role Stress Scales

4.7 Social Role Stress

Overall, the mean OQ-45.2 social role stress subscale score per group was 10.09 (SD = 4.43) for active duty cyber operators, 8.81 (SD = 4.13) for cyber civilian/contractor operators, and 9.33 (SD = 4.59) for the noncyber control group. An analysis of variance assessing between group differences was significant, $F = 5.26$, $p < .01$. Subsequent mean comparisons using t-tests for equal variance (Bonferroni t) were significant when comparing mean scores between active duty cyber operators and cyber civilian/contractor operators ($t = 1.28$, $p \leq 0.01$) and between active duty cyber operators and the noncyber control group ($t = 0.76$, $p \leq 0.02$). There was no significant difference between cyber civilian/contractor operators and the noncyber control group ($t = -0.52$, $p \leq 0.59$).

The number and percentage of those who scored 12 or more on the OQ-45.2 social role distress subscale (a discretionary cut-off score set by the authors of the OQ-45.2 as indicative of high social role distress) were 121 (34.38%) for active duty cyber operators, 39 (26.71%) for cyber civilian/contractor operators, and 217 (28.78%) for the noncyber control group (see Figure 2). Subsequent chi-square tests for between group differences in the frequency of those who reported high social role distress showed significant differences between active duty cyber operators and cyber civilian/contractor operators ($\chi_2 = 2.78$, $p < 0.10$) and between active duty cyber operators and the noncyber control group ($\chi_2 = 3.54$, $p < 0.06$). However, there was no significant difference between cyber civilians/contractor operators and the noncyber control group ($\chi_2 = 0.26$, $p < 0.61$).

5.0 DISCUSSION

5.1 Sources of Occupational Stress

A qualitative analysis of cyber operator survey responses revealed the operators' top occupational stressors to include the following:

- *Leadership-organizational issues*
    - leadership not effectively communicating job requirements
    - inexperienced leadership not understanding operational needs and realities
    - multiple demands coming from various agencies with conflicting requests regarding task prioritization
    - lack of understanding how warfighting role contributes or impacts broader operational missions
- *Operational tempo, workload, and low manning*
    - insufficient manning to fulfill job tasks/requests
    - frequent, short-notice, line-of-sight taskings by supervisors
    - frequent 50+-hour work weeks
- *Nature of work and training*
    - inadequate tools for training or to implement newer methodologies
    - lack of experienced operators to provide training
    - keeping up with rapidly changing/evolving technology

Such stressors are common across cyber warfare operating units and frequently cited as the main sources for occupational stress.

However, there was a difference between active duty and civilian/contractor cyber warfare operators related to top sources of stress. Active duty cyber warfare operators cited shift work as a significant contributor to their occupational stress. They also reported the effects of shift work to be disruptive to meeting family and domestic life obligations and marital/family relationships. Active duty cyber warfare operators engaged in shift work were more likely to report disruptions in family life care than their civilian/contractor cyber warfare colleagues. Further examination into this difference points to a distinction in work schedules within units that are predominantly active duty compared to those that are predominantly civilian/contractor. In almost every case, units that were predominantly active duty worked a 24/7 shift rotation, while units that were predominantly civilian/contractor cyber warfare operators worked a standard day or extended day shift. Furthermore, active duty cyber warfare operators reported to work on average 51 or more hours per week, while civilian operators reported working within a 40-hour work week. Alternately, civilian/contractor cyber warfare operators were more likely to report stressors related to job security and financial concerns. Given an atmosphere of fiscal cutbacks and budget constraints, civilian/contractor operators appear to be more worried about whether current or future budget constraints will result in a reduction in pay or loss of job.

The results of the analyses also revealed that occupational stressors cited by active duty and civilian cyber warfare operators are different from those in the USAF noncyber control group. The noncyber control group cited stressors centered on career progression, fitness, and occupational morale. There was, however, a common stressor shared by the AF control group and civilian/contractor cyber operators regarding financial concerns. Both groups reported stress related to the risk of government-related fiscal constraints and potential impact of force shaping and manpower cuts on their livelihood. Current and future force reductions appear to be a top concern for those in support/logistics units. The results suggest that, in general, civilian/contractor and active duty support/logistics personnel have concerns over their job security and economic disposition, which is a concern likely shared by many across the nation in both current military and civilian job markets.

5.2 Facets of Occupational Burnout

A high level of emotional exhaustion is a likely sign of distress in response to emotionally demanding work. The results of the study reveal that one out of every four active duty cyber warfare operators reports high levels of exhaustion. Specifically, on the MBI-GS, emotional exhaustion is measured by the depletion of emotional energy due to work-related stress. Findings also indicate that, in general, active duty cyber warfare operators report higher levels of exhaustion compared to their civilian/contractor counterparts and noncyber active duty airmen from support/logistics units. Although this study was not specifically designed to render cause-effect conclusions, the prevalence of key stressors reported by active duty cyber warfare operators points to high ops tempo, shift work, leadership/organizational management issues, and nature of work as contributors to higher exhaustion.

A high level of cynicism is a likely sign of a strong negative work attitude, which may or may not be related to emotional exhaustion. The results of the study reveal that active duty personnel (whether from the cyber warfare operator group or the non-cyber group of support/logistics airmen) report higher scores on cynicism than civilian/contractor cyber warfare operators. Specifically, on the MBI-GS, cynicism is measured by the degree of indifference or a distant attitude towards work (e.g., a declining sense of enthusiasm for work). In general, one out of every 10 active duty airmen who responded to the survey reported having high levels of cynicism. It is difficult to determine the cause for high levels of cynicism. Regardless, the results of the study suggest active duty leadership is challenged to inspire, motivate, and cultivate a positive perception among airmen regarding their occupational duties and assignment. The results of this study provide a benchmark for leadership for gauging how effective their efforts are at creating a positive work attitude among their subordinates for the future.

A low level of professional efficacy is a likely sign that one perceives having a minimal degree of accomplishment at work. The results of this study indicate that most cyber warfare operators (active duty and civilian/contractor) have a reasonable level and healthy sense of professional efficacy. Specifically, on the MBI-GS, professional efficacy is measured by the sense of one’s competence and accomplishments at work. There was no difference between groups in this area. It is interesting to note that in light of emotional exhaustion and cynicism among active duty cyber warfare operators, such measures did not appear to impact their sense of professional efficacy.

5.3 Clinical and Social Role Distress

As mentioned previously, emotional distress is a commonly used phrase to refer to an unpleasant emotional state characterized by negative emotional, behavioral, physical, and cognitive changes in functioning. Given the sensitive nature of cyber warfare operations, it is critical to military commanders to gauge the levels of emotional distress experienced among airmen directly engaged in such operations. Furthermore, a clinical level of emotional distress is a general cluster of emotional-behavioral symptoms that place one at an elevated risk for anxiety, depression, or adjustment-related difficulties.

The results of the study reveal active duty cyber warfare operators report higher levels of general clinical stress and are more likely to report clinical distress than noncyber airmen from support/logistics units. However, there was no significant difference between active duty and civilian cyber warfare operators regarding levels of clinical stress. This would suggest the operational environment of cyber warfare operations elevates the risk for emotional distress and that active duty cyber warfare operators are at elevated risk for clinical distress when compared with noncyber active duty airmen from support/logistics units. As mentioned earlier, although this study was not specifically designed to render cause-effect conclusions, the prevalence of key stressors reported by cyber warfare operators points to the following as contributors to higher levels of distress: high ops tempo, shift work, leadership/organizational management issues, and the nature of work.

As mentioned, social role distress is a sense of discomfort and distress associated with one's social roles at work and home. The results of the study reveal high levels of social role distress among each group of participants who responded to the survey. The balancing of work with domestic obligations is a challenge that many face on a daily basis, regardless of their duty position. However, study findings indicate that active duty cyber warfare operators are significantly more likely to report high levels of social role distress than civilian/contractor cyber warfare operators and airmen from support/logistics unit.

5.4 Line and Medical Management Recommendations

Regardless of the study limitations, a significant percentage of active duty cyber warfare operators assessed reported higher levels of emotional exhaustion and cynicism. As a result, active duty cyber warfare units are likely to benefit from increased leadership engagement and mental health care discussed below. Although medical interventions will likely improve the overall emotional health of cyber warfare operators, it is ill-advised to rely solely on medical personnel to manage this issue. In the absence of operational leadership engagement, medical and psychological treatments will merely be treating the symptoms and not addressing salient causes of organizational and individual stress.

5.4.1 Leadership Recommendations. The findings in this study suggest that many of the symptoms of burnout and distress reported by cyber warfare operators are of an operational nature and can be addressed by leadership through altering organizational factors and scheduling. Among these factors are the following:

- optimizing work/rest cycles to reduce incidence of fatigue
- implementing more stable shift durations and rotation schedules to minimize disruptions to circadian rhythm adjustment and capability of meeting social role requirements in one's domestic life (e.g., optimal scheduling would use a clockwise (morning-afternoon-night) rotational schedule; limiting shift duration to 8 hours, and allowing 3 days of recuperation after night shifts)
- addressing existing manning shortages before expanding operations to reduce or mitigate the need for operators to work over 50+ hours a week
- implementing routine, periodic rest breaks during shift to optimize operators' capacity for long-term vigilance
- incorporating physical fitness programs centered on core strength to enhance resilience
- allowing operators adequate opportunity for training necessary to cultivate and sustain efficacy in this new mission area (e.g., consider blended learning [11] as an approach to training; blended learning is an effective technique in training individuals that incorporates a blend of teaching and hands-on training)

It is also recommended that leadership effectively communicate requirements; intervene when cyber operators have to respond to multiple and at times conflicting taskers from various agencies demanding immediate response; and inspire, motivate, and educate cyber operators on how their efforts have a positive and critical impact on USAF missions for achieving and sustaining cyberspace superiority across the globe. Leadership may also want to improve morale by educating cyber operators on how their efforts also contribute to USAF aviation and special duty operations. Having a "big picture" perspective regarding how one's efforts are valued and influence other areas critical to the USAF may help to engender a positive work attitude that may mitigate, to some degree, the impact of other operational stressors associated with sustaining around-the-clock operations. Lastly, having commanders incorporate experienced mental health providers into their morale and team building meetings may help raise awareness to early signs of burnout and distress.

5.4.2 Medical Recommendations. Although operational interventions can make great strides in reducing the number of occupational stressors, this study reveals that for the cyber community, the overall impact of stress manifests in a predominantly psychological manner. This finding points to the requirement for medical support from mental health providers.

Implementing strategies to strengthen the relationship between medical/mental health organizations and the cyber arena is critical to optimizing the use of available medical/mental health interventions. Experienced medical/mental health providers dedicated to this mission area would constitute the core element in strengthening this relationship. Assigning specific medical and mental health providers as liaisons with cyber organizations would allow them to interact and educate both leaders and operators on operational stress and interventions and may help increase access and utilization for mental health care by those who need it.

Although finding medical personnel to permanently embed themselves within this unit may be difficult to implement, the following are recommendations for experienced medical/mental health providers who can do weekly to monthly visits to these units:

- offer monthly sleep hygiene classes to improve the sleep hygiene skills of the personnel in these units
- offer monthly stress management classes to improve adaptation and coping skills
- consider offering monthly spouse educational groups that incorporate education on the cyber warfare operator profession, stress management, couples communication, and other topics of interest
- offer stress inoculation training, which would include preparing the operators with real information on the types of images, stress, and demands they will experience and ways to cope with it
- offer periodic assessments utilizing the MBI-GS to provide continued feedback to cyber leadership on the occupational burnout on their units
- offer periodic assessments utilizing the OQ-45.2 to assess for unit level of distress for feedback to unit leadership

The above recommendations would require a commitment from both leadership and the medical and mental health teams.

5.5 Assumptions and Limitations of the Study

This study assumes that since the survey device is anonymous and nonattributable in nature, all respondents are answering truthfully, with no hidden agendas. It is also assumed that the sample group is sufficient to represent the target audience, and nonrespondents would answer no differently than those who volunteered to do so. Finally, the study assumes that there are no unwarranted assumptions in the survey instrument itself.

Organizationally formalized in 2008, the cyber operations career field is still remarkably new to the USAF. Thus, there are many facets of cyberspace warfare research that have not been conducted, and very few studies have been completed that examine the effects of the new career field on those who are selected to serve in it.

The temporal nature and the survey methodology of the study suggest limited concern for the external validity, and/or generalizability, of its findings. The foundation of generalizability is probability sampling, and the study relies upon the convenience sampling of cyber operators who were available to complete the survey during specific time periods. In addition, this study cannot account for any shifts in operations tempo (up or down) that may have occurred during the period of survey data collection. All cyber units will be surveyed again at a later date to confirm study findings and to assess for changes in the prevalence of occupational burnout following implementation of remedial and preventative initiatives.

Since the intent of this study is to not diagnose mental illness but to screen for indicators, this study is not able to account for preexisting conditions, whether physical or psychological, unless self-reported within the survey. This does point to another study limitation associated with the survey methodology, which does not allow for definitive judgments about the psychological disposition and service needs of cyberspace operators. The implicit assumption of those endorsing high levels of emotional exhaustion and distress is they need mental health care or medical intervention to mitigate such unpleasant conditions that can negatively affect performance. However, further studies are needed to address functional impairment to assess the validity of this implicit assumption.

This study is descriptive in nature and raises awareness to the most concerning sources of stress, as well as prevalence of burnout and clinical distress among such a critical group of operators. This information is helpful for medical and line leadership in their management of such operators for optimizing performance and sustaining health. However, it is important to bear in mind the methodology of this study does not allow for definitive cause-effect conclusions. The sources of stress and levels of burnout and emotional distress appear to be related, but specific cause-effect conclusions are not supported by this study. As a result, caution must be given in how the results are interpreted. The study may help to inform leadership and medical management decisions and guide thought processes on strategies for improving health and performance, but further research is needed to fully extrapolate or identify specific causes for higher levels of exhaustion, cynicism, and distress. More specifically, research is needed to explore leadership concerns related to whether or not the nature of the offensive cyber mission is associated with high levels of stress.

6.0 CONCLUSIONS

USAF cyber warfare operations have emerged as critical assets to all Air Force operations. Cyber warfare operations will continue to grow in importance as information technology accelerates exponentially. Line leadership and medical providers should remain vigilant to the impact that technology, shift work, and operational tempo may have on the psychological health of the human cyber warfare operator. While medical and psychological factors should remain key considerations in the selecting and maintaining of a healthy cyber warfare operator work force, operational leaders should seek out opportunities to minimize occupational stressors in this mission area. Leadership will need to focus on promoting expertise and continuity of experience through improved rates of retention. They will also have to identify and implement measures to increase tasking efficiency and reduce occupational stress. With the medical resources available to advise commanders and assist individuals, dynamic policy and leadership can significantly reduce the factors that induce occupational burnout and clinical distress.

7.0 REFERENCES

1. Franz T. The Air Force and cyber warfare: concepts, strategies, and current efforts. Presented at the Air Force Symposium 2008: Cyberspace. Maxwell AFB, AL, 15-17 Jul 2008. Accessed 11 July 2012 from http://www.au.af.mil/au/awc/cyberspace/read.html.

2. Franz T. The cyber warfare professional: realizations for developing the next generation. Air and Space Power Journal 2011 Summer; 26(2):87-99. Accessed 11 July 2012 from http://www.airpower.au.af.mil/airchronicles/apj/2011/2011-2/2011_2.asp.

3. Xie Z, Wang A, Chen B. Nurse burnout and its association with occupational stress in a cross-sectional study in Shanghai. J Adv Nurs 2011; 67(7):1537-46.

4. Bawa N, Kaur R. Occupational stress and burnout among police officers. Indian Journal of Community Psychology 2011; 7(2):362-72.

5. Wu S, Zhu W, Li H, Wang Z, Wang M. Relationship between job burnout and occupational stress among doctors in China. Stress & Health 2008; 24(2):143-9.

6. Senter A, Morgan RD, Serna-McDonald C, Bewley M. Correctional psychologist burnout, job satisfaction, and life satisfaction. Psychological Services 2010; 7(3):190-201.

7. Onder C, Basim N. Examination of developmental models of occupational burnout using burnout profiles of nurses. J Adv Nurs 2008; 64(5):514-23.

8. Chairman of the Joint Chiefs of Staff. Information operations. Washington, DC: Chairman of the Joint Chiefs of Staff; 2012 Nov 27. Joint Publication 3-13.

9. Maslach C, Jackson SE, Leiter MP. Maslach burnout inventory manual, 3rd ed. Palo Alto, CA: Consulting Psychologists Press; 1996.

10. Lambert MJ, Hansen NB, Umpress V, Lunnen K, Okiishi J, Burlingame GM, et al. Administration and scoring manual for the OQ-45.2. Stevenson, MD: American Professional Credentialing Services, LLC; 2000.

11. Wu JH, Tennyson RD, Hsia TL. A study of student satisfaction in a blended e-learning system environment. Computers & Education 2010; 55(1):155-64.

LIST OF ABBREVIATIONS AND ACRONYMS

CND	computer network defense
CNE	computer network exploitation
MBI-GS	Maslach Burnout Inventory-General Schedule
OQ-45.2	Outcome Questionnaire-45.2
SD	standard deviation
USAF	United States Air Force